CLAIMS

1. A cryptography acceleration chip, comprising:

a classification engine configured to receive a complete IP packet and determine what keys are needed to encrypt or decrypt the packet.

2. The chip of claim 1, wherein said determination is accomplished by parsing fields in a header of the packet to determine a flow to which the packet belongs.

3. The chip of claim 2, wherein said flow has one or more associated keys for encrypting or decrypting the packet.

4. The chip of claim 1, wherein said engine supports all necessary modes for IPSec security processing.

5. The chip of claim 1, wherein said chip further comprises an internal local memory.

6. The chip of claim 1, wherein said chip further comprises an external local memory.

7. The chip of claim 5, wherein said memory is one of a DRAM, SSRAM, and CAM.

8. The chip of claim 6, wherein said memory is one of a DRAM, SSRAM, and CAM.

9. The chip of claim 8, wherein said memory is one of a DRAM and an SSRAM, and said chip further comprises a hash-based lookup table.

10. The chip of claim 9, wherein said hash-based lookup table has a two layer structure.

11. The chip of claim 10, wherein said two layer hash-based lookup table comprises a hash map table and a classification entry table.

12. The chip of claim 11, wherein said hash map table is sparse.

13. The chip of claim 12, wherein an output of said hash map table comprises indexes into the classification entry table.

14. The chip of claim 13, wherein said classification entry table holds a copy of classification match fields and additional match tag information.

15. The chip of claim 5, wherein said memory is a CAM.

16. The chip of claim 15, wherein said CAM is configured to hold 128 entries.

17. The chip of claim 16, wherein each of said entries comprises a match field of 106 bits, said match field including a 2 bit match type code, and a match tag of 32 bits.

18. The chip of claim 15, wherein said chip is configured to conduct a de-correlation process.

19. The chip of claim 1, wherein said packets comprise short packets.

20. The chip of claim 1, wherein said packets comprises voice-over-IP packets.

21. A method for accelerating cryptography processing of data packets, the method comprising:

receiving a plurality of complete data packets on a cryptography acceleration chip;

processing the data packets with a classification engine to determine what keys are needed to encrypt or decrypt the packets.

22. The method of claim 21, wherein said determination is accomplished by parsing fields in a header of each of the packets to determine a flow to which each of the packets belongs.

23. The method of claim 22, wherein said flow has one or more associated keys for encrypting or decrypting the packet.

24. The method of claim 21, wherein said engine supports all necessary modes for IPSec security processing.

25. The method of claim 24, further comprising a RAM-based hash-based classification match lookup process.

26. The method of claim 25, wherein said hash-based match lookup has two levels.

27. The method of claim 26, wherein said two levels comprise a hash map lookup and a classification entry lookup.

28. The method of claim 27, wherein an output of said hash map lookup indexes into the classification entry table.

29. The method of claim 24, further comprising a CAM-based classification.

30. The method of claim 29, wherein said CAM-based classification is conducted using a bit mask to reflect binarized range specifiers from an IPSec policy rule set.

31. The method of claim 30, wherein a binarization and de-correlation processing precede said CAM-based classification .

32. The method of claim 21, wherein said packets comprise short packets.

33. The method of claim 21, wherein said packets comprises voice-over-IP packets.

34. A network line card, comprising:

a cryptography acceleration chip comprising,

a classification engine configured to receive a complete IP packet and determine what keys are needed to encrypt or decrypt the packet;

a local central processing unit connected with said chip;

a local memory connected with said chip;

a network interface unit connected with said chip; and

a system interface unit connected with said chip.

35. The line card of claim 34, wherein said local memory is one of DRAM and SSRAM.

36. The line card of claim 34, wherein said local memory is CAM.

37. A network service module, comprising:

a cryptography acceleration chip comprising,

a classification engine configured to receive a complete IP packet and determine what keys are needed to encrypt or decrypt the packet;

a local central processing unit connected with said chip;

a local memory connected with said chip; and

a system interface unit connected with said chip.

38. The line card of claim 37, wherein said local memory is one of DRAM and SSRAM.

39. The line card of claim 37, wherein said local memory is CAM.

40. A network communication device, comprising:

a central processing unit;

a system memory;

a network interface unit;

a cryptography acceleration chip comprising,

a classification engine configured to receive a complete IP packet and determine what keys are needed to encrypt or decrypt the packet.

an internal bus that connects the central processing unit, the system memory, the network interface unit, and the cryptography acceleration chip.

41. The device of claim 40, wherein the internal bus is a high speed switching matrix.

42. The device of claim 40, wherein said chip resides on a network line card.

43. The device of claim 42, wherein said line card further comprises:

a local central processing unit connected with said chip;

a local memory connected with said chip;

a network interface unit connected with said chip; and

a system interface unit connected with said chip.

44. The device of claim 40, wherein said chip resides on a network service module.

45. The device of claim 44, wherein said service module further comprises:

a local central processing unit connected with said chip;

a local memory connected with said chip; and

a system interface unit connected with said chip.